About CyberScore™

CyberScore is aligned to the UK Cyber Essentials Plus scheme and can dramatically reduce the likelihood of falling victim to cybercrime.

What is CyberScore™ and what does it do?

CyberScore™ gathers data about your organisation and interprets it to present a view of your security posture. It's simple: you download the CyberScore™ software, allow it to scan your network and produce your very own, peer-rated security score, along with a Get Well Plan and a CyberScore™ certificate.

What does my CyberScore™ mean?

You receive a numerical score from 0 to 10 along with an alphabetical suffix from A to F. For example, you might score 5.6C. The numerical score is a measure of your internal security – how tough you are on the inside. The alphabetical suffix is a measure of your external security – how hard your perimeter is to the outside world.

What are the benefits of using CyberScore™?

CyberScore™ aims to prevent harm being done to your organisation, either directly or via third parties. CyberScore™ does this by giving you a view of your security posture - that is, how you look to someone seeking to attack your IT infrastructure - and creating a plan to allow you to fix things quickly. If you or your partners are running obsolete software - we'll let you know. If you're running supported software that is missing lots of security fixes, we'll flag it and include it in your Get Well Plan. We'll let you know where all of your vulnerabilities are, which ones are most important, either because of their nature or their prevalence. And we'll tell you what to do about them, hopefully before someone else, who cares less about your wellbeing, does.

What's actually going on? How does it work?

CyberScore™ uses a scanner to gather vulnerability data from every device it can see on your network. It interprets the data, encrypts it and sends it to our secure data centre for analysis. Our algorithms calculate your security score, identify the areas of greatest concern, and present the data back to you as actionable information via the CyberScore™ portal.

What exactly does CyberScore™ scan?

CyberScore™ automatically detects devices (computers, routers, gateways, mobile devices etc.) on your network. If there are devices connected to your network, CyberScore™ can locate them and, if you don't know what your network looks like or what your IP addresses are, we can automatically detect them for you. Once we have found the computers on your network, we can carry out detailed inspections of them to check for vulnerabilities. Finally, we can turn the process around and scan you from the outside, to assess your perimeter security.

Where is my data held?

XQ houses all data within Ark Data Centres – the UK's most efficient and secure data hosting centre. Ark is Pan Government Accredited (PGA) data centre in the UK that contractually guarantees power usage efficiency (PUE). Ark is ISO27001 certified and XQ Cyber will shortly attain this certification. Only you get to see your data. You have control over your account administration rights and the assignment of credentials to all networks and hosts in your organisation. If a third party such as an insurer, an investor or a supply chain operator has asked you to undertake a CyberScore™, you can elect to share your CyberScore™ with that third party. The third party will see your CyberScore™ – but they will not see any underlying technical or vulnerability data.

How can I get the most from CyberScore™ ?

Getting the most from CyberScore™ is easy: first, scan far and wide, and as often as you can. That way you'll get as complete a picture of your IT systems as possible. By scanning regularly, ideally every month, you'll stay on top of new vulnerabilities as they appear. Second, scan in-depth by providing CyberScore™ with full access to your computers. These detailed checks will offer a far more accurate and detailed picture of where your strengths and weaknesses may be and allow us to offer far more meaningful advice. Don't worry, it's easy to set up.

What does my Cyber Essentials advisory mean?

CyberScore™ automatically assesses your alignment to the Cyber Essentials Plus scheme. At present we're only able to offer an advisory recommendation, that is, whether we think you would pass or fail certification. As soon as we are able to offer Cyber Essentials Plus certification, we'll let you know.

What about security?

Your data is safe. In fact, we think it's probably safer with us than it is with you. It is doubly encrypted in transit, and is housed within an IT environment designed by security cleared professionals with years of experience breaking into such systems. CyberScore's™ infrastructure is routinely security tested and is monitored 24x7x365.

Are my credentials safe?

Unless you are a regular purchaser of security consultancy and penetration testing, entering login details (usernames and passwords) may feel a little daunting. Rest assured: your login data is doubly-encrypted in transit on the way to our high-security data centre, and is stored there in such a way that only you can use it - we've taken steps to ensure that not even we can see it! Nobody from XQ will ever contact you asking for your credentials.

What do I need to run CyberScore™?

The CyberScore scanner requires 4GB of RAM (although more is better) and 20GB of disk space. CyberScore™ is available as a virtual appliance for use within VMware vSphere or Microsoft HyperV environments. The appliance is available for VMware ESXi 5.1 (and Workstation 9) onwards and for Microsoft HyperV.

What should I expect during a scan?

As CyberScore™ scans your network, your Antivirus software may prompt an alert on each device. This is completely normal. Any IP phones may ring (once per phone) as they are discovered. The scan itself will take several hours, depending on the size of your network.

http://www.netutils.com/partners/cyberscore/